UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,487	08/16/2001	Edward W. Kohler JR.	12221-006001	3664

26161 7590 01/19/2005

FISH & RICHARDSON PC
225 FRANKLIN ST
BOSTON, MA 02110

EXAMINER	
ISMAIL, SHAWKI SAIF	
ART UNIT	**PAPER NUMBER**
2155	

DATE MAILED: 01/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,487	KOHLER ET AL.	
	Examiner	Art Unit	
	Shawki S Ismail	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *8-16-2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 August 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are presented for examination.

Applicant's claim for priority is acknowledged.

References in applicant's IDS form 1449 have been considered.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference character(s) mentioned in the description: (for example with regards to figure 1, there is mention of reference characters 16 and 18, which are not in Fig. 1). Corrected drawing sheets are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC §102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

4. Claims 1-12, 15-20, are rejected under 35 U.S.C. 102(e) as being anticipated by **Cox et al.**, (Cox) U.S. Patent No. **6,738,814.**

5. As to claim 1, Cox teaches a method of protecting a victim site against a denial of service attack, the method comprises:

receiving network packets with faked source addresses (col. 3, lines 55-56);

receiving from the victim site a notification that the victim site is under an attack (col. 3, lines 23-29); and

sending queries to data collectors to request information from at least some of the data collectors, the information to determine the source of suspicious network traffic being sent to the victim (Fig. 3, col. 3, line 55 – col. 4, line 15, and col. 3, lines 35-45).

6. As to claim 2, Cox teaches the method of claim 1 wherein the network packets from the attacker have faked, random source addresses that change with time, and sending queries further comprises:

sending queries to the data collectors for information based on victim destination address (col. 3, line 55 – col. 4, line 15 and col. 3, lines 35-45).

7. As to claim 3, Cox teaches the method of claim 1 wherein based on collected information the method further comprises:

determining what data centers are performing the spoofing on the victim (col. 3, line 55 – col. 4, line 15).

8. As to claim 4, Cox teaches the method of claim 3 wherein determining is performed by a control center, and determining further comprising: sending data to/from a gateway device that is associated with the victim center (col. 3, line 55 – col. 4, line 15).

9. As to claim 5, Cox teaches the method of claim 4 wherein the gateway identifies the network address of the victim, via a message to the control center (col. 4, lines 41-61).

10. As to claim 6, Cox teaches the method of claim 5 wherein the message is sent over a hardened network (col. 4, lines 41-61).

11. As to claim 7, Cox teaches the method of claim 5 wherein message indicates the type of attack (col. 3, lines 35-45 and col. 4, lines 41-61).

12. As to claim 8, Cox teaches the method of claim 1 wherein the attacker is behind a gateway (col. 3, line 55 – col. 4, line 15).

13. As to claim 9, Cox teaches the method of claim 8 wherein if the attacker is behind a gateway, the control center issues a request to the gateway that the attacker is behind to block the attacking traffic (col. 3, line 55 – col. 4, line 15).

14. As to claim 10, Cox teaches the method of claim 8 wherein if the attacker is behind a gateway, the gateway that the attacker is behind selectively discards traffic that appears to be malicious traffic and that contains the victim destination address (col. 3, line 55 – col. 4, line 15).

15. As to claim 11, Cox teaches the method of claim 1 wherein if the attacker is not behind a gateway, the control center queries the data collectors to provide information about possible locations of the attackers (col. 3, line 55 – col. 4, line 15).

16. As to claim 12, Cox teaches the method of claim 1 wherein if the attacker is not behind a gateway, the method further comprises:

contacting administrators at locations involved in attack to have the administrators take action to filter out packets with the destination address (col. 4, lines 10-15).

17. As to claim 15, Cox teaches a method of protecting a victim site against a denial of service attack, the method comprises:

receiving packets with faked, random source addresses (col. 3, lines 55-56);

receiving a notification that the victim data center is under an attack, from a gateway disposed near the victim site (col. 3, lines 23-29);

sending queries to data collectors to request information from data collectors that have examined network traffic with the victim destination address (Fig. 3, col. 3, line 55 – col. 4, line 15, and col. 3, lines 35-45); and

determining the data center or centers involved in the attack on the victim by analyzing collected information from the data collectors (col. 3, line 55 – col. 4, line 15).

18. As to claim 16, Cox teaches the method of claim 15 wherein the control center also includes a communication process to send data to/from a gateway device that is disposed with the victim center (col. 4, lines 41-61).

19. As to claim 17, Cox teaches the method of claim 16 wherein if the attacker is behind a gateway, the control center issues a request to the gateway to block the attacking traffic (col. 3, line 55 – col. 4, line 15).

20. As to claim 18, Cox teaches the method of claim 17 wherein if the attacker is behind a gateway, the gateway selectively discards traffic that appears to be malicious traffic and that contains the victim destination address (col. 3, line 55 – col. 4, line 15).

21. As to claim 19, Cox teaches the method of claim 15 wherein if the attacker is not behind a gateway, the method comprises:

contacting administrators at locations involved in attack to filter out packets having the destination address (col. 4, lines 10-15).

22. As to claim 20, Cox teaches a system to thwart denial of service attacks on a victim, comprises:

a plurality of monitors dispersed throughout a network, the monitors collecting statistical data on network traffic (col. 3, lines 35-45);

a control center coupled to the plurality of data collectors, the control center executing a computer program product stored on a computer readable medium, comprising instructions for causing a computer to:

receive from the victim site a notification that the victim data center is under an attack (col. 3, lines 55-56); and

send queries to data collectors to request information from data collectors, the information used to determine the source of suspicious network traffic being sent to the victim (Fig. 3, col. 3, line 55 – col. 4, line 15, and col. 3, lines 35-45);

a gateway device that passes network packets between the network and the victim site, the gateway disposed to protect the victim site, and being coupled to the control center (col. 2, lines 46-58).

Claim Rejections - 35 USC § 103

23. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

24. Claim 13 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Cox et al.,** (Cox) U.S Patent No. **6,738,814** and in view of **Hill et al.,** (Hill) U.S. Patent No. **6,088,804.**

25. As to claim 13 and 14, Cox teaches a method for blocking denial of service and address spoofing attacks on a network. However, Cox does not explicitly teach wherein the attacks are classified into categories based on the severity that they cause to the network.

Hill teaches a system and method for adaptively responding to computer network security attacks. Hill further teaches classifying attacks based on the severity of the attack on the network (Fig. 3, col. 2; lines 53-60; col. 6, lines 9-22).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate Hill's classification of the severity of attacks into the

invention of Cox in order minimize the load on the computer network. Displaying attack information would help the network manager prioritize the severity of the attacks so that it spend less time countering lesser threats and more time countering severe threats (col. 2, lines 47-53).

Conclusion

26. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shawki S Ismail whose telephone number is 571-272-3985. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hosain Alam can be reached on 571-272-3978. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shawki Ismail
Patent Examiner
January 12, 2004

HOSAIN ALAM
SUPERVISORY PATENT EXAMINER